THE GROUPS OF POINTS ON ABELIAN VARIETIES OVER FINITE FIELDS

SERGEY RYBAKOV

Abstract. Let A be an abelian variety with commutative endomorphism algebra over a finite field k. The k-isogeny class of A is uniquely determined by a Weil polynomial f_A without multiple roots. We give a classification of the groups of k-rational points on varieties from this class in terms of Newton polygons of $f_A(1-t)$.

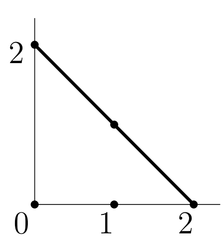
1. Introduction

Let A be an abelian variety of dimension g over a finite field $k = \mathbb{F}_q$, and let $A(k)$ be the group of k-rational points on A. Tsfasman [Ts85] classified all possible groups $A(k)$, where A is an elliptic curve (see the English exposition in [TsVN07, 3.3.15]). Later the same result was independently proved in [Ru87] and [Vo88] using [Sch87]. Xing obtained a similar classification when A is a supersingular simple surface [Xi94] and [Xi96]. In this paper such a description is obtained for the groups of k-rational points on abelian varieties with commutative endomorphism algebra.

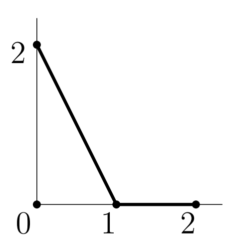
For an abelian group H we denote by H_ℓ the ℓ-primary component of H. Let $A(k) = \oplus_\ell A(k)_\ell$. We associate to $A(k)_\ell$ a polygon of special type.

Definition 1. Let $0 \le m_1 \le m_2 \le \cdots \le m_r$ be nonnegative integers, and let $H = \oplus_{i=1}^r \mathbb{Z}/\ell^{m_i}\mathbb{Z}$ be an abelian group of order ℓ^m. The *Hodge polygon* $\mathrm{Hp}_\ell(H, r)$ *of a group* H is the convex polygon with vertices $(i, \sum_{j=1}^{r-i} m_j)$ for $0 \le i \le r$. It has $(0, m)$ and $(r, 0)$ as its endpoints, and its slopes are $-m_r, \dots, -m_1$.

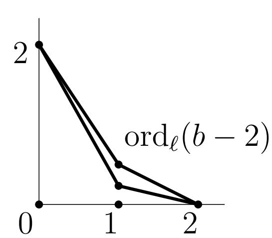
Note that Hodge polygon of a group depends on a choice of r, but the zero slope of $\mathrm{Hp}_\ell(A(k)_\ell, r)$ is not interesting, and we can use the most convenient choice of r. Mostly we need the case $r = 2g$, and write $\mathrm{Hp}_\ell(H) = \mathrm{Hp}_\ell(H, 2g)$ (here we assume that H can be generated by $2g$ elements). For example, let $g = 1$, and $H = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$, then $\mathrm{Hp}_\ell(H, 2)$ is a straight line (see Picture 1). Let $H = \mathbb{Z}/\ell^2\mathbb{Z}$ be cyclic, then $\mathrm{Hp}_\ell(H, 2)$ has a zero slope (see Picture 2).



Pic. 1



Pic. 2



Pic. 3

1991 *Mathematics Subject Classification.* 14K99, 14G05, 14G15.
Key words and phrases. abelian variety, the group of rational points, finite field, Newton polygon, Hodge polygon.
Supported in part by RFBR grants no. 07-01-00051, 07-01-92211 and 08-07-92495.

Note also that isomorphism class of H depends only on $\mathrm{Hp}_\ell(H)$. For a polynomial $P \in \mathbb{Z}[t]$ we denote by $\mathrm{Np}_\ell(P)$ the Newton polygon of P with respect to ℓ (see Section 3 for the precise definition). The aim of this paper is to prove the following theorem.

Theorem 1. *Let A be an abelian variety over a finite field with Weil polynomial f_A (see Section 2 for the definition of Weil polynomial). Suppose f_A has no multiple roots (i.e. endomorphism algebra $\mathrm{End}^\circ(A)$ is commutative). Let G be an abelian group of order $f_A(1)$. Then G is a group of points on some variety in the isogeny class of A if and only if $\mathrm{Np}_\ell(f_A(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_\ell)$ for any prime number ℓ.*

As an example, we prove the following corollary of Theorem 1. Originally it was proved in [Ts85]. Later the same result was independently proved in [Ru87] and [Vo88] using [Sch87].

Corollary 1. *Let $N = 1 - b + q$ be the order of $B(k)$ for an elliptic curve B. Then $G = B(k)$ satisfies the following conditions.*

(1) *If $b \neq \pm 2\sqrt{q}$, then $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$, where $N = n_1 n_2$, and n_1 divides $b-2$ and n_2.*
(2) *If $b = \pm 2\sqrt{q}$, then $G \cong (\mathbb{Z}/n_1\mathbb{Z})^2$, and $N = n_1^2$.*

If a finite commutative group G satisfies (1) or (2), then there exists an elliptic curve B' isogenous to B such that $B'(k) \cong G$.

Proof. If $b \neq \pm 2\sqrt{q}$, then f_B has no multiple roots. Fix a prime ℓ. Let $B(k)_\ell \cong \mathbb{Z}/\ell^{m_1}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_2}\mathbb{Z}$, and let $m_1 \leq m_2$. Since $f_B(1-t) = t^2 + (b-2)t + (1-b+q)$, we have by Theorem 1 that $m_1 \leq \mathrm{ord}_\ell(b-2)$ (see Picture 3). Equivalently, ℓ^{m_1} divides $b-2$, and the first case follows. The second case is obvious since F acts on T_ℓ as multiplication by $b/2 = \pm\sqrt{q}$. Conversely, if G satisfies (1), then the existence of an elliptic curve B' with $B'(k) \cong G$ follows from Theorem 1 combined with the inequality $m_1 \leq \mathrm{ord}_\ell(b-2)$. □

Remark 1. Originally the Tsfasman theorem relies on the Waterhouse classification of isogeny classes of elliptic curves [Wa69] and has 6 cases. We make the statement shorter, but it becomes a little different. For example, for a supersingular curve B with commutative endomorphism algebra it is not immediately clear that $B(k)$ is cyclic modulo 2-torsion.

Corollary 1 allows us to construct an example of an isogeny class with the following properties:

(1) The Weil polynomial f has multiple roots;
(2) not any abelian group G of order $f(1)$ such that $\mathrm{Np}_\ell(f(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_\ell)$ for any prime number ℓ is a group of points on some variety from the isogeny class.

Indeed, take $f(t) = (t-3)^2$. Then by Corollary 1 for any A from the isogeny class $A(\mathbb{F}_9) \cong (\mathbb{Z}/2\mathbb{Z})^2$. It follows that the isogeny class does not contain an elliptic curve, whose group of points is cyclic.

The author is grateful to M.A. Tsfasman and Yu.G. Zarhin for their attention to this work and to reviewer for providing useful corrections and comments on the paper.

2. Preliminaries

Throughout this paper k is a finite field $\mathbb{F}_q$ of characteristic p. Let A and B be abelian varieties over k. It is well known that the group $\mathrm{Hom}(A,B)$ of k-homomorphisms from A to B is finitely generated and torsionfree. We use the following notation: $\mathrm{Hom}^\circ(A,B) = \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^\circ(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The algebra $\mathrm{End}^\circ(A)$ contains the Frobenius endomorphism F, and its center is equal to $\mathbb{Q}[F]$. Thus $\mathrm{End}^\circ(A)$ is commutative if and only if $\mathrm{End}^\circ(A) = \mathbb{Q}[F]$.

Let A be an abelian variety of dimension g over k, and let $\bar{k}$ be an algebraic closure of k. For a natural number m denote by A_m the kernel of multiplication by m in $A(\bar{k})$. Let $A[m]$ be the group subscheme of A, which is the kernel of multiplication by m. By definition $A_m = A[m](\bar{k})$. Let $T_\ell(A) = \varprojlim A_{\ell^r}$ be the Tate module, and $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the corresponding vector space over $\mathbb{Q}_\ell$. If $\ell \neq p$, then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. The Frobenius endomorphism F of A acts on the Tate module by a semisimple linear operator, which we also denote by $F : T_\ell(A) \to T_\ell(A)$. The characteristic polynomial

$$f_A(t) = \det(t - F|T_\ell(A))$$

is called a *Weil polynomial of* A. It is a monic polynomial of degree $2g$ with rational integer coefficients independent of the choice of prime $\ell \neq p$. It is well known that for isogenous varieties A and B we have $f_A(t) = f_B(t)$. Moreover, Tate proved that the isogeny class of abelian variety is determined by its characteristic polynomial, that is $f_A(t) = f_B(t)$ implies that A is isogenous to B. The polynomial f_A has no multiple roots if and only if the endomorphism algebra $\mathrm{End}^\circ(A)$ is commutative (see [WM69]).

If $\ell = p$, then $T_p(A)$ is called a *physical Tate module*. In this case, $f_A(t) = f_1(t)f_2(t)$, where $f_1, f_2 \in \mathbb{Z}_p[t]$, and $f_1(t) = \det(t - F|T_p(A))$. Moreover $d = \deg f_1 \leq g$, and $f_2(t) \equiv t^{2g-d} \mod p$ (see [De78]).

We say that $\varphi : B \to A$ is an *ℓ-isogeny*, if degree of φ is a power of ℓ. The following lemma is well known, but we prove it here for the sake of completeness.

Lemma 1. *If $\varphi : B \to A$ is an isogeny then $T_\ell(\varphi) : T_\ell(B) \to T_\ell(A)$ is a $\mathbb{Z}_\ell$-linear embedding commuting with the action of the Frobenius endomorphisms and if T denotes its image then*

$$F(T) \subset T \quad \text{and} \quad T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell. \tag{1}$$

Conversely, if $T \subset T_\ell(A)$ is a $\mathbb{Z}_\ell$-submodule such that (1) *holds, then there exists an abelian variety B over k, and an ℓ-isogeny $\varphi : B \to A$ such that $T_\ell(\varphi)$ induces an isomorphism $T_\ell(B) \cong T$.*

Proof. The first part is obvious. The second part can be proved as follows. First, (1) implies that there exists $k \in \mathbb{Z}$ such that $\ell^k T_\ell(A) \subset T$. Further, note that $T_\ell(A)/\ell^k T_\ell(A) \cong A_{\ell^k}$. Hence the group $T/\ell^k T_\ell(A)$ can be considered as a subgroup in $A_{\ell^k} \subset A(\bar{k})$. Moreover, since $F(T) \subset T$ it follows that $T/\ell^k T_\ell(A)$ is invariant under the action of the Frobenius, and thus defines a certain group subscheme G of A. If $\ell \neq p$, we define $B = A/G$. If $\ell = p$, there is the canonical decomposition $A[p^k] = G_r \oplus G_l$, where G_r is reduced and $G_r(\bar{k}) = A_{p^k}$, and $G_l(\bar{k}) = 0$ [De78]. In this case, we define $B = A/(G \oplus G_l)$. It is clear that B is defined over k, and $A \cong B/G'$, where G' is reduced and $G'(\bar{k}) = T_\ell(A)/T$. This gives a desired isogeny $\varphi : B \to A$. □

3. The groups of points

Let $Q(t) = \sum_i Q_i t^i$ be a polynomial of degree d over $\mathbb{Q}_\ell$, and let $Q(0) = Q_0 \neq 0$. Take the lower convex hull of the points $(i, \mathrm{ord}_\ell(Q_i))$ for $0 \leq i \leq d$ in $\mathbb{R}^2$. The boundary of this region without vertical lines is called *the Newton polygon* $\mathrm{Np}_\ell(Q)$ *of* Q. Its vertices have integer coefficients, and $(0, \mathrm{ord}_\ell(Q_0))$ and $(d, \mathrm{ord}_\ell(Q_d))$ are its endpoints.

Let E be an injective endomorphism of $T_\ell(A)$, and let $H = T_\ell(A)/ET_\ell(A)$ be its cokernel, which is a finite ℓ-group. Define the *Hodge polygon of the endomorphism* E as the Hodge polygon $\mathrm{Hp}_\ell(H, \mathrm{rk}\, T_\ell(A))$ of the group H. We need the following simple result.

Proposition 1. *The Hodge polygon $\mathrm{Hp}_\ell(A(k)_\ell, \mathrm{rk}\, T_\ell(A))$ is equal to the Hodge polygon of $1 - F$.*

Proof. Since $A(k)_\ell$ is finite, there exists a positive integer N such that $A(k)_\ell \subset A_{\ell^N}$. Clearly, $A(k)_\ell = \ker(1-F : A_{\ell^N} \to A_{\ell^N})$. Apply $1-F$ to the short exact sequence:

$$0 \to T_\ell(A) \xrightarrow{\ell^N} T_\ell(A) \to A_{\ell^N} \to 0.$$

By snake lemma we get:

$$0 = \ker(1-F : T_\ell(A) \to T_\ell(A)) \to A(k)_\ell \to T_\ell(A)/(1-F)T_\ell(A) \xrightarrow{0} T_\ell(A)/(1-F)T_\ell(A).$$

Thus $A(k)_\ell \cong T_\ell(A)/(1-F)T_\ell(A)$, and the proposition follows. $\square$

We see that the group $A(k)_\ell$ depends only on the action of F on the Tate module $T_\ell(A)$. In particular, order of $A(k)$ is $f_A(1)$. Thus we reduced our task to the following linear algebra problem. We are given a $\mathbb{Q}_\ell$-vector space V of finite positive dimension d and an invertible linear operator $E : V \to V$, whose characteristic polynomial $f(t) = \det(E - t|V)$ lies in $\mathbb{Z}_\ell[t]$. We want to describe all finite commutative groups (up to isomorphism) of the form T/ET, where T is an arbitrary E-invariant $\mathbb{Z}_\ell$-lattice of rank d in V. We solve this problem under the additional assumption that f has no multiple roots.

The next statement establishes a connection between the Hodge polygon of an endomorphism and the Newton polygon of its characteristic polynomial.

Theorem 2. [Ke09, 4.3.8][BO, 8.40] *Let E be an injective endomorphism of a free $\mathbb{Z}_\ell$-module of finite rank. Let $f(t) = \det(E - t|V)$ be its characteristic polynomial. Then $\mathrm{Np}_\ell(f)$ lies on or above the Hodge polygon of E, and these polygons have same endpoints.*

Recall that if $\ell = p$, then $f_A(t) = f_1(t)f_2(t)$, and $f_2(t) \equiv t^{2g-d} \mod p$. Thus the only slope of $\mathrm{Np}_p(f_2(1-t))$ is zero, and $\mathrm{Np}_p(f_A(1-t))$ equals to $\mathrm{Np}_p(f_1(1-t))$ up to this zero slope.

Corollary 2. *Let A be an abelian variety A with Weil polynomial f_A. Then $\mathrm{Np}_\ell(f_A(1-t))$ lies on or above $\mathrm{Hp}_\ell(A(k)_\ell)$, and these polygons have same endpoints $(0, \mathrm{ord}_\ell(f_A(1))$ and $(2g, 0)$.*

Now we are ready to solve our linear algebra problem.

Theorem 3. *Let V be a $\mathbb{Q}_\ell$-vector space of positive finite dimension d, and let $E : V \to V$ be an invertible linear operator such that the characteristic polynomial $f(t) = \det(E - t|V)$ lies in $\mathbb{Z}_\ell[t]$. Suppose f has no multiple roots. Let G be an abelian group of order ℓ^m, where $m = \mathrm{ord}_\ell(f(0))$. If $\mathrm{Np}_\ell(f)$ lies on or above $\mathrm{Hp}_\ell(G, d)$, then there exists an E-invariant $\mathbb{Z}_\ell$-lattice T of rank d in V such that $T/ET \cong G$.*

Corollary 3. *We keep the notation of theorem 3. Suppose f has no multiple roots. Then the group G is isomorphic to T/ET for some E-invariant $\mathbb{Z}_\ell$-lattice T of rank d in V if and only if $\mathrm{Np}_\ell(f)$ lies on or above $\mathrm{Hp}_\ell(G, d)$, and these polygons have same endpoints $(0, \mathrm{ord}_\ell(f(0))$ and $(d, 0)$.*

Proof of theorem 3. Since f has no multiple roots, there is an isomorphism of $\mathbb{Q}_\ell$-vector spaces $V \cong \mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$ such that E becomes multiplication by t in $\mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$. Let x be an image of t in $\mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$, and let $R = \mathbb{Z}_\ell[x]$ be the $\mathbb{Z}_\ell$-subalgebra of $\mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$ generated by x. Then R is a $\mathbb{Z}_\ell$-lattice in $\mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$; in particular, the natural map $R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to \mathbb{Q}_\ell[t]/f(t)\mathbb{Q}_\ell[t]$ is an isomorphism of $\mathbb{Q}_\ell$-vector spaces. We have to find an R-submodule $T \subset R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of $\mathbb{Z}_\ell$-rank d such that x acts on T with Hodge polygon $\mathrm{Hp}_\ell(G, d)$.

Suppose $G = \oplus_{i=1}^d \mathbb{Z}/\ell^{m_i}\mathbb{Z}$, where $m_1 \le m_2 \le \cdots \le m_d$ (recall that m_i may be zero for some i). First we construct certain elements $v_0, \ldots, v_d \in R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let us put $M(0) = 0$, and $M(s) = \sum_{i=1}^s m_i$

for $s \geq 1$. Let $f(t) = \sum_{i=0}^{d} a_i t^i$. We let

$$v_s = \frac{a_d x^s + \sum_{j=1}^{s} a_{d-j} x^{s-j}}{\ell^{M(s)}},$$

in particular, $v_d = f(x)/\ell^m = 0$. Second, we define T as the $\mathbb{Z}_\ell$-submodule of $R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ generated by d elements $v_0, \ldots, v_{d-1}$. Note that $v_0, v_2, \ldots, v_{d-1}$ have different degrees viewed as polynomials in x (and all degrees are strictly less than d), and hence form a basis of T over $\mathbb{Z}_\ell$. In particular, T is a free $\mathbb{Z}_\ell$-module of rank d. Notice that $v_0 = a_d = (-1)^d$. In particular, T contains $\mathbb{Z}_\ell \cdot 1$.

Now we prove that T is an R-submodule of $R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The point $(d - s, M(s))$ is a vertex of $\mathrm{Hp}_\ell(G, d)$. By assumption $\mathrm{Np}_\ell(f)$ lies on or above $\mathrm{Hp}_\ell(G, d)$; thus $(d - s, M(s))$ is not higher than $\mathrm{Np}_\ell(f)$. It follows that $\ell^{M(s)}$ divides a_{d-s}, and

$$u_s = \frac{a_{d-s}}{\ell^{M(s)}} \cdot 1 \in \mathbb{Z}_\ell \cdot 1 \subset T,$$

thus for $s \geq 1$

$$xv_{s-1} = \ell^{m_s}(v_s - u_s) \in \ell^{m_s} T. \tag{2}$$

This proves that $xT \subset T$.

Recall that, $v_0 = a_d = (-1)^d$; clearly $m = \mathrm{ord}_\ell(\det E) = \mathrm{ord}_\ell(a_0)$; thus $u_d = a_0/\ell^m$ is invertible in $\mathbb{Z}_\ell$, and

$$v_1 - u_1, \ldots, v_d - u_d = -u_d$$

is a basis of the free $\mathbb{Z}_\ell$-module T. This gives us the natural surjective map $\mathbb{Z}^d \to T/xT$. It follows from (2) that this map factors through a surjective map $G \to T/xT$. We conclude that $T/xT \cong G$, since orders of both groups are equal to ℓ^m. □

Proof of theorem 1. The "if" part follows from Corollary 2. Let us prove the "only if" part.

For a given prime number ℓ and an abelian variety A' isogenius to A we let $V = V_\ell(A')$ and $E = 1 - F$. If $\ell \neq p$, we let $f(t) = f_A(1 - t)$, and if $\ell = p$, we let $f(t) = f_1(1 - t)$. By Theorem 3 there exists an E-invarint lattice T in V such that $T/ET \cong G_\ell$. Clearly, T is F-invariant, and by Lemma 1 there exists an abelian variety B' and an ℓ-isogeny $B' \to A'$ such that $T_\ell(B') \cong T$. By Proposition 1 we have $G_\ell \cong B'(k)_\ell$.

Let $\ell_1, \ldots, \ell_s$ be the set of prime divisors of $f_A(1)$. It follows that there exists a sequence of isogenies

$$B = B_s \xrightarrow{\varphi_s} B_{s-1} \to \ldots \xrightarrow{\varphi_2} B_1 \xrightarrow{\varphi_1} A$$

such that $\varphi_i : B_i \to B_{i-1}$ is an ℓ_i-isogeny and

$$B_i(k)_{\ell_i} \cong G_{\ell_i}.$$

Since φ_i is an ℓ_i-isogeny, $T_\ell(B_i) \cong T_\ell(B_{i-1})$ for any $\ell \neq \ell_i$. Thus $B(k) \cong G$. □

4. Noncommutative endomorphism algebras

If $\mathrm{End}\, A$ is not commutative then we may apply the following construction. Let $f_A = \prod_{j=1}^{s} f_j$, where all f_i are polynomials with integer coefficients, and f_j divides f_{j-1}. Suppose f_j has no multiple roots for $1 \leq j \leq s$. Let G_j be a family of abelian ℓ-groups for $1 \leq j \leq s$ such that $\mathrm{Np}_\ell(f_j(1 - t))$ lies on or above $\mathrm{Hp}_\ell(G_j, \deg f_j)$. By Theorem 3 and Lemma 1, we can construct modules T_j and an abelian variety B with Tate module $T_\ell(B) = \oplus T_j$ such that $B(k)_\ell \cong \oplus G_j$. We have the following conjecture.

Conjecture 1. *Let $f_A = \prod_{j=1}^{s} f_j$, where f_j divides f_{j-1}, and suppose that f_j has no multiple roots for $1 \le j \le s$. If $\deg f_j \le 2$ for all j, then $A(k)_\ell \cong \oplus G_j$, where G_j are ℓ-primary abelian groups such that $\mathrm{Np}_\ell(f_j(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_j, \deg f_j)$ for all $1 \le j \le s$.*

This conjecture is proved in [Xi94] for simple abelian surfaces. However, there is an example of the group of points on an abelian variety A with $\deg f_1 = 3$, and $\deg f_2 = 1$ such that this group is not a direct sum of two groups G_1 and G_2 such that $\mathrm{Np}_\ell(f_j(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_j, \deg f_j)$ for $j = 1, 2$. Let us consider the Weil polynomial $f(t) = (t^2 - 2t + 9)(t + 3)^2$, and let A be an abelian surface such that $f_A = f$. Then $f(1-t) = (t^2 + 8)(t-4)^2$. Let v_1, v_2, v_3, v_4 be a basis of $V_2(A)$ such that $(1-F)v_1 = 2v_2$, $(1-F)v_2 = -4v_1$, $(1-F)v_3 = 4v_3$, and $(1-F)v_4 = 4v_4$. Let T be the $\mathbb{Z}_2$-submodule of $V_2(A)$ generated by $u_1 = v_1 + v_3, u_2 = -4v_2 + 4v_3, u_3 = v_2 + v_4$, and $u_4 = 4v_1 + 2v_4$. By Lemma 1 there exists an abelian surface B such that $T_2(B) \cong T$. We claim that

$$B(\mathbb{F}_9)_2 \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Indeed,

$$\begin{gathered}(1-F)u_1 = 4u_1 + 2u_3 - u_4 \in T \\ (1-F)u_2 = 16u_3 \in T \\ (1-F)u_3 = 4u_1 - u_2 + 4u_3 \in T \\ (1-F)u_4 = 8u_1 \in T.\end{gathered}$$

Theorem 1 and Conjecture 1 allows one to classify the groups of points on simple abelian surfaces. However the author does not know even a conjectural classification of groups of points on nonsimple surfaces.

References

[BO] Berthelot P., Ogus A., Notes on crystalline cohomology, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[De78] Demazure M., Lectures on p-divisible groups, Lecture notes in mathematics 302, Springer-Verlag, Berlin, 1972.

[Ke09] Kedlaya K., p-adic differential equations, Cambridge University Press, to appear, web draft (30.09.2009) available at http://www-math.mit.edu/~kedlaya/papers/pde.pdf

[Ru87] Rück H.-G., A note on elliptic curves over finite fields. Math. Comp. 1987, 49 no. 179, 301–304.

[Sch87] Schoof R., Nonsingular plane cubic curves over finite fields, J. Combin. Theory Ser. A, 1987, 46 no. 2, 183–211.

[Ts85] Tsfasman M. A., The group of points of an elliptic curve over a finite field, Theory of numbers and its applications, Tbilisi, 1985, 286-287.

[TsVN07] Tsfasman M., Vladut S., Nogin D., Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI, 2007.

[Vo88] Voloch J. F., A note on elliptic curves over finite fields, Bull. Soc. Math. France, 1988, 116 no. 4, 455–458.

[Wa69] Waterhouse W., Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup., 1969, 4 serie 2, 521–560.

[WM69] Waterhouse W., Milne J., Abelian varieties over finite fields, Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969, 53–64.

[Xi94] Xing Ch., The structure of the rational point groups of simple abelian varieties of dimension two over finite fields, Arch. Math., 1994,63, 427–430.

[Xi96] Xing Ch., On supersingular abelian varieties of dimension two over finite fields, Finite Fields Appl., 1996, 2, no. 4, 407–421.

Poncelet laboratory (UMI 2615 of CNRS and Independent University of Moscow)

Institute for information transmission problems of the Russian Academy of Sciences
E-mail address: rybakov@mccme.ru, rybakov.sergey@gmail.com